Abstract

Detecting attacks against computer systems by automatically detecting signatures based on predetermined characteristics of the intrusion. One aspect looks for commonalities among a number of different network messages, and establishes an intrusion signature based on those commonalities. Data reduction techniques, such as a hash function, are used to minimize the amount of resources which are necessary to establish the commonalities. In an embodiment, signatures are created based on the data reduction hash technique. Frequent signatures are found by reducing the signatures using that hash technique. Each of the frequent signatures is analyzed for content, and content which is spreading is flagged as being a possible attack. Additional checks can also be carried out to look for code within the signal, to look for spam, backdoors, or program code.